IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA, v. TOYE TUTIS and JAZMIN VEGA, Defendants.	HONORABLE JEROME B. SIMANDLE Crim. No. 14-699 (JBS) **OPINION**

APPEARANCES:

Diana Vondra Carrig, Assistant U.S. Attorney
Howard Weiner, Assistant U.S. Attorney
Jonathan Peck, Assistant U.S. Attorney
OFFICE OF THE U.S. ATTORNEY
401 Market Street
Camden, NJ 08101

J. Michael Farrell, Esq.
718 Arch Street
Suite 402N
Philadelphia, PA 19106
Attorney for Defendant Toye Tutis

Troy A. Archie, Esq.
21 Route 130 South
Cinnaminson, NJ 08077
Attorney for Defendant Jazmin Vega

SIMANDLE, Chief Judge:

I. INTRODUCTION

The Second Superseding Indictment herein arises from a long-running investigation into an allegedly large scale drug trafficking and money laundering organization. More

specifically, the First Superseding Indictment, filed March 16, 2016, charges Defendants Toye Tutis (hereinafter, "Defendant Tutis" or "Toye Tutis") and Jazmin Vega (hereinafter "Defendant Vega" or "Vega"), among others, with conspiring to distribute kilogram quantities of heroin and cocaine throughout southern New Jersey, and other crimes related to such drug distribution. The charges were refined in a Second Superseding Indictment filed September 14, 2016, and Defendants Tutis and Vega are the sole remaining defendants. [See generally Docket Item 339.]

In the present motions, Defendant Tutis now moves to suppress evidence obtained by electronic surveillance, on the grounds that the Government unconstitutionally obtained the evidence through the use of a cell-site simulator that was unlawfully authorized under a communications data warrant on October 14, 2014. [See Docket Items 322, 331, 350.] Defendant Vega seeks a bill of particulars pursuant to Fed. R. Crim. P. 7(f). The Government opposes all motions.

For the reasons that follow,[1] Defendant Tutis's motion to suppress evidence obtained by a cell-site simulator pursuant to the October 14, 2014 communications data warrant and Defendant Vega's motion for a bill of particulars will be denied.

[1] The Court conducted oral argument relative to the pretrial motions of all defendants on September 8, 2016 [see Docket Item 337], supplemented by a hearing concerning the cell-site simulator issues on September 27, 2016. [see Docket Item 352.]

II. FACTUAL AND PROCEDURAL BACKGROUND

A. Investigation Background and CDW Authorization

The charges contained in the Superseding Indictment and Second Superseding Indictment stem from a long-running investigation conducted jointly by federal, state, and local law enforcement officers, targeting an alleged drug-trafficking organization in Atlantic City and the surrounding southern New Jersey region. (See Walsh Aff. at ¶¶ 5-6.) This Court has thoroughly discussed the background of this case in United States v. Tutis, No. 14-699, 2016 WL 885044 (D.N.J. Mar. 8, 2016) [Docket Item 264], and will assume the reader's familiarity with that discussion.

As relevant here, the Atlantic County Prosecutor's Office (hereinafter, the "ACPO") obtained a series of wiretaps, authorized by the Honorable Bernard E. DeLury (hereinafter, "Judge DeLury") and supported by the affidavits of Detective Jason E. Dorn (hereinafter, "Detective Dorn"), on cellular telephones known to be used by Defendant Tutis. (See Gov't Opp'n to Def. Tutis's First Set of Pretrial Motions at 7; see also Dorn Sept. 19, 2014 Aff. (Gov't Ex. 2); Dorn Sept. 26, 2014 Aff. (Gov't Ex. 3).) On September 19, 2014, the ACPO obtained its first "roving" wiretap authorization (BED-ATL-21-WT-2014) to intercept communications over the cellular telephone of Jewell Tutis. After a few days of intercepting communications pursuant

to that wiretap, Detective Dorn (and others) determined that Toye Tutis had used a specific cellular telephone in connection with his alleged drug distribution, namely 424-646-1761, and requested roving wiretap authorization to intercept communications of Toye Tutis. (See Dorn Sept. 26, 2014 Aff. at ¶¶ 3-5.)

After reviewing the Affidavit, Judge DeLury issued the requested wiretap on September 26, 2014 (BED-ATL-22-WT-14 & BED-ATL-153-CDW-14). Then, in the matter at issue in the present opinion, on October 14, 2014, Detective Dorn applied for and Judge DeLury approved a Communications Data Warrant (BED-ATL-162-CDW-14) (hereinafter "the Tutis CDW") which authorized the use of "wireless interrogation equipment" that was "capable of retrieving wireless instrument identification information" of cell phones utilized by Tutis. (See Ex. 1, ¶ 7K, ¶ 9, to Gov't Sur-Reply.) The "wireless interrogation equipment" referred to in the Tutis CDW is a cell-site simulator device ("CSS"). (See Gov't Sur-Reply at 1.) In his Affidavit for the Tutis CDW, Detective Dorn explains that he applied for permission to use the CSS because he believed that Tutis "ha[d] demonstrated a willingness to change" his cell phone number, and would "continue to change" numbers "with the purpose to thwart interception by members of law enforcement." (Id. at ¶ 3A.) Additionally, Tutis "used multiple telephone facilities at the

same time with a purpose to thwart detection or interception by law enforcement, and ha[d] clearly evidenced his intention to continue to change wireless telephone facilities, or devices for that purpose." (Id.) As a result, the data obtained by the CSS would "assist law enforcement in ascertaining the additional [cell phones] utilized by Toye Tutis." (Id. at ¶ 8K.)

Regarding the scope of the use of the CSS, the Affidavit explains that the CSS device would only retrieve the Electronic Serial Number ("ESN"), Mobile Telephone Number ("MSISDN"), and International Mobile Subscriber Identification Number ("IMSI") from any phones associated with Tutis. (Id. at ¶ 9.) The "only function" of the device regarding this investigation was to identify those data points, as it was "not [to be] used to obtain any written or oral communications." (Id. at ¶ 4A, ¶ 9.) To obtain the data, the ACPO would "utiliz[e] the equipment in close proximity" to Tutis "at different geographical locations," and since the ESN, MSISDN, and ISMI "are unique," Tutis's cell phones "may be identified by a process of elimination." (Id. at ¶ 4A.) ACPO would then confirm Tutis's usage of each cell phone by "analysis of the Call Detail Records and subscriber information" for the cell phones identified by the CSS. The CSS, in other words, would not itself identify Tutis' cell phone but it would instead canvass all cell phones within close proximity to Tutis at one location and then do so again at other

known Tutis locations, yielding lists of identifying data for each vicinity's cell phones. Then by "process of elimination" the detectives could focus upon the common cell phone number(s) that showed up at each Tutis location, which logically would be highly probably possessed by Tutis, and thus lead to the identification of a new Tutis cell phone. The CSS, as used in this case, would not be directed at a Tutis phone, since his new numbers were unknown when the device would be used to canvass the vicinities. Judge DeLury granted ACPO's request to use "electronic equipment to retrieve certain cellular telephone information" for 30 days on a 24 hour, 7 day per week basis." (See Tutis CDW Order, Ex. 1 to Gov't Sur-Reply.) Judge DeLury also approved another CDW based upon an affidavit reciting the same information regarding the use of the "electronic equipment," on December 2, 2014 (BED-ATL-190-CDW-14). (See Ex. 2 to Gov't Sur-Reply.) The latter CDW did not result in obtaining usable electronic data according to the Government. (Gov't Sur-Reply at 2.)

B. December 9, 2014 Search Warrants, December 10, 2014 Indictment, and Arrests

Thereafter, on December 9, 2014, federal law enforcement agents obtained federal search warrants for approximately seven properties throughout southern New Jersey, all of which bore some claimed relation to the alleged drug trafficking

organization. (See Gov't Opp'n to Defendant Tutis's First Set of Pretrial Motions at 32; see also Walsh Aff. at ¶ 7.)

Then, on December 10, 2014, a federal grand jury returned a two-count Indictment charging certain defendants with conspiring to traffic in cocaine, heroin, and crack cocaine, and certain others with conspiring to conceal and/or disguise the proceeds of this unlawful activity, followed by the First and Second Superseding Indictments as above. During the execution of the search and arrest warrants, officers seized additional evidence of drug trafficking and money laundering, including more than one kilogram of crack cocaine, lesser amounts of powder cocaine and heroin, eight firearms, two tasers, more than forty cellular telephones, a bulletproof vest, and in excess of $100,000 in cash. (See Gov't Opp'n to Defendant Tutis's First Set of Pretrial Motions at 32-33.)

C. Defendant's First Set of Pretrial Motions

This Court, in its March 8, 2016 Opinion addressing Defendants' first set of pretrial motions, denied Defendant Tutis's motion to suppress the wire and electronic conversations captured under the September 26, 2014 wiretap because it found that Judge DeLury had a substantial basis to find that Detective Dorn's Affidavit, viewed in its entirety, demonstrated a "fair probability" of Toye Tutis's involvement in criminal activity. See Tutis, 2016 WL 885044 at *11. The undersigned also denied

Defendant Tutis's request that the Court conduct a Franks hearing regarding omissions in the September 26, 2014 wiretap Affidavit, because he made no showing that Detective Dorn knowingly, intentionally, and/or recklessly made a false statement. Id. at *12. The decision denying a Franks hearing has been reconsidered at hearings on September 27, 2016 and October 13, 2016, and a Franks hearing commenced on October 17, 2016 that will be the subject of a forthcoming separate Opinion addressing all objections to the September 26, 2014 wiretap.[2]

III. MOTION OF TOYE TUTIS TO SUPPRESS EVIDENCE OBTAINED THROUGH CELL-SITE SIMULATOR PURSUANT TO WARRANT

In moving to suppress the wire and electronic conversations captured under various Tutis wiretaps, Defendant Tutis, relying on eight separate bases, claims that the supporting Affidavits filed in the Superior Court lacked probable cause; thus, any fruits of the Tutis wiretaps should be suppressed. The Government opposes suppression, principally on the grounds that Judge DeLury had a substantial basis for authorizing the Tutis wiretaps based on the totality of the circumstances. The Court addresses only one of the bases in this Opinion–-suppression

[2] At this point, nine of the indicted defendants have pleaded guilty to the drug trafficking conspiracy or other drug distribution charges. These defendants are Kareem Taylor, Philip Horton, Talib Tiller, Ronald Douglas Byrd, John Wellman, and Francisco Rascon-Muracami, Tejohn Cooper, Tozine Tiller, and Kabaka Atiba.

based on the use of a cell-site simulator which Judge DeLury permitted in the communications data warrant of October 14, 2014.

A. Standard for Suppression

The traditional Fourth Amendment principles that apply to property searches govern probable cause determinations under the federal and/or state wiretap statutes. See United States v. Tehfe, 722 F.2d 1114, 1118 (3d Cir. 1983); see also 18 U.S.C. § 2518(3) (federal wiretap statute); N.J.S.A. § 2A:156A-10 (state wiretap statute). The same Fourth Amendment standards govern finding probable cause for a wiretap order and for a search warrant. United States v. Tehfe, 722 F.2d 1114, 1118 (3d Cir. 1983). Under these principles, a finding of probable cause requires a "'fair probability'" of criminal activity, based upon the totality of the circumstances. United States v. Bond, 581 F.3d 128, 139 (3d Cir. 2009) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)). The reviewing court need not determine whether probable cause actually existed, but only whether there was "a 'substantial basis' for finding probable cause." United States v. Jones, 994 F.2d 1051, 1054 (3d Cir. 1993). Stated differently, the issuing court must "make a practical, common-sense decision" concerning whether the circumstances set forth in the supporting Affidavit, "including the 'veracity' and 'basis of knowledge' of the persons supplying the hearsay

information," demonstrate "a fair probability" that the authorization will result in evidence of a crime. Id. at 238-39.

A reviewing court must afford great deference to the probable cause finding of an issuing court. See United States v. Hodge, 246 F.3d 301, 305 (3d Cir. 2001); United States v. Jones, 994 F.2d 1051, 1055 (3d Cir. 1993). As a result, the probable cause determination of an issuing court will be upheld so long as the supporting documents provided a substantial basis for the initial probable cause decision.[3] See United States v.

---

[3] Title III of the Omnibus Crime Control and Safety Street Act of 1968 empowers a judge to enter an ex parte order to authorize interception of wire communications, if the judge determines on the basis of the facts submitted by the application that:

> (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit [a drug-trafficking offense]; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; (d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

18 U.S.C. §§ 2518(3)(a)-(d). The New Jersey Wiretapping and Electronic Surveillance Control Act, which governed the wiretap at issue here, contains analogous provisions, and specifically authorizes the issuance of a wiretap, if the judge finds probable cause to believe that:

> a. [t]he person whose communication is to be intercepted is engaging or was engaged over a period of time as a part of a continuing criminal activity or is committing, has or had committed or is about to commit an offense as provided in section 8 of P.L.1968, c.409 (C.2A:156A-8); b. [p]articular

Hodge, 246 F.3d 301, 305 (3d Cir. 2001); United States v. Jones, 994 F.2d 1051, 1055 (3d Cir. 1993) ("[T]he resolution of doubtful or marginal cases in this area should be largely determined by the preference to be accorded to warrants."). This deferential standard "does not mean that reviewing courts should simply rubber stamp" the authorizing judge's conclusions, United States v. Tehfe, 722 F.2d 1114, 1117 (3d Cir. 1983) (citing United States v. Ventresca, 380 U.S. 102, 108 (1965)), but it does counsel that "resolution of doubtful or marginal cases ... be largely determined by the preference ... accorded to warrants." United States v. Jones, 994 F.2d 1051, 1055 (3d Cir. 1993) (citing Ventresca, 380 U.S. at 109). In other words, the standard encourages slight doubts concerning the propriety

---

> communications concerning such offense may be obtained through such interception; c. [n]ormal investigative procedures with respect to such offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ; d. [e]xcept in the case of an application meeting the requirements of subsection g. of section 9 of P.L.1968, c.409 (C.2A:156A-9), the facilities from which, or the place where, the wire, electronic or oral communications are to be intercepted, are or have been used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by, such individual; e. [t]he investigative or law enforcement officers or agency to be authorized to intercept the wire, electronic or oral communication are qualified by training and experience to execute the interception sought; and f. [i]n the case of an application, other than a renewal or extension, for an order to intercept a communication of a person or on a facility which was the subject of a previous order authorizing interception, the application is based upon new evidence or information different from and in addition to the evidence or information offered to support the prior order, regardless of whether such evidence was derived from prior interceptions or from other sources.

N.J.S.A. § 2A:156A-10.

of the wiretap authorization to be resolved in favor of the issuing court. Id. Finally, "[s]tatements in an affidavit may not be read in isolation—the affidavit must be read as a whole." United States v. Kaplan, 526 F. App'x 208, 212 (3d Cir. 2013).

B. Tutis's Motion to Suppress Evidence Obtained By a Cell-Site Simulator Pursuant to Communications Data Warrant of October 14, 2014

Tutis argues that the wiretap evidence should be suppressed because it was illegally obtained by prior use of a Stingray, or cell-site simulator, pursuant to an allegedly defective communications data warrant issued by Judge DeLury on October 14, 2014, and that an evidentiary hearing should be held to probe into the use of the device and the technical process employed.[4] The Court did not convene a testimonial hearing, because Tutis did not identify issues of fact material to his motion. United States v. Hines, 628 F.3d 101, 105 (3d Cir. 2010) ("A motion to suppress requires an evidentiary hearing only if ... there are disputed issues of material fact that will affect the outcome of the motion to suppress."). The Court, however,

[4] Following oral argument on Defendant's second set of pretrial motions, on September 12, 2016, the Court issued an Order Concerning Defendants' Various Pretrial Motions, which specifically directed the Government to (a) file a sur-reply to the [CSS] suppression motion, and (b) provide discovery as to "when and how the [CSS] was used to gather the evidence which Defendant Tutis seeks to suppress; and . . . whether the [CSS] was utilized to identify the existence of an electronic device within [his] home . . . ." [See Docket Item 338.]

required the Government to provide additional information about the use of the cell-site simulator, which was received on September 15, 2016, and a hearing addressed these issues on September 27. As discussed below, the Court finds that no Fourth Amendment or state law violations occurred in this particular case, and will deny the motion to suppress regarding the use of the cell-site simulator.

1. Background Regarding Cell Site Simulator in this Case

As discussed further below, a cell-site simulator ("CSS") is a device used by law enforcement to simulate a cell tower in order to obtain information related to the presence of cell phones in an area proximate to a suspect's physical presence. By gathering identifying signals from many cell phones in proximity, and then gathering new samples from other locations where the suspect is present at other times, a law enforcement officer can narrow the list of identified cell phones to those that watch the suspect's locations and eliminate the many that do not appear to follow the suspect from one place to another. By such process of elimination, the officer can deduce the phone numbers which may belong to the suspect, and then match those few numbers to numbers known to be involved in the illegal transactions. Thus, from an array of cell phone identification data at various locations where the suspect is known to be when the CSS is used, the officer can by process of elimination and

deduction narrow the field to the data associated with the suspect's cell phone or phones. As one federal court recently described it:

> [B]y simulating a cell site, the device causes or forces cell-phones in an area to send their signals – with all the information contained therein – to the cell-site simulator. Once the cell phones in the area send their signals to the cell-site simulator, the device captures a vast array of information, including, but not limited to, the cell phones' electronic serial number ("ESN") or international mobile subscriber identification ("IMSI"). A cell phone need only be on for the cell-site simulator to capture the cell phone's ESN and IMSI; the cell phone need not be "in use."

In the Matter of the Application of the of Am. for an Order Relating to Telephones Used by Suppressed, No. 15-0021, 2015 WL 6871289 at *2 (N.D. Ill. Nov. 9, 2015). Despite the prevalent use of cell-site simulators by law enforcement, there are few reported cases regarding its use. See, e.g., id.; United States v. Lambis, No. 15-734, 2016 WL 3870940 (S.D.N.Y. July 12, 2016); United States v. Rigmaiden, No. 08-814, 2013 WL 1932800 (D. Az. May 8, 2013); In re U.S. for an Order Auth. the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747 (S.D. Tex. 2012).

In the instant action, ACPO investigators knew that Tutis was using cell phones to further his criminal activities, but they were unable to determine his specific cell phone numbers or other electronic identification information. (Ex. 1 to Gov't Sur-Reply.) As a result, they sought and obtained judicial authorization to use the CSS. The October 14, 2014

Communications Data Warrant ("CDW") (No. BED-ATL-162-CDW-14), which Judge DeLury issued and which authorized the use of the CSS for 30 days, resulted in the use of a CSS on three dates: October 16, November 5, and November 10. (Gov't Sur-Reply at 2.) A second CDW was obtained on December 2, 2014, but that did not result in any information being collected that was used in this case. (Id.) Furthermore, the October 14, 2014 CDW was a "hybrid" warrant, in that it combined a request for authorization to use the CSS with a request that the telephone service provider ("TSP") be ordered to provide subscriber information to law enforcement. (Gov't Sur-Reply at 3, n. 3; Ex. 1.)

On the three aforementioned dates, law enforcement took the CSS to multiple separate locations where Tutis was known to be, conducted surveillance to establish that he was present at a particular location, and then used the CSS at that location to capture electronic signals (IMSI and mobile station ID) emanating from cell phones in that area. (Id. at 4.) The Government explains that the CSS was used to "canvass" several locations where Tutis was located, in an attempt to determine the IMSI and/or mobile station ID of the phone(s) he had in his possession. (Id. at 4, n. 4.) The CSS was "used in the vicinity of a building at which Tutis was observed, or based upon prior knowledge was believed to be located at the time of canvassing."

(Id. at 14.) More specifically, the CSS "emitted a signal omnidirectionally, so that it could be picked up by cell phones in the general vicinity," and "received signals emanating from any phone(s) inside buildings and any other telephones in the area that were turned on and sending electronic signals to the nearest cell tower." (Id.) After using the device at several locations, law enforcement determined the common IMSIs and subpoenaed the TSPs for subscriber names and information of common IMSIs and mobile station IDs, and looked for connections to Tutis.

2. The Fourth Amendment Implications of the Use of the Cell-Site Simulator

Tutis argues that (1) the Government should have obtained a search warrant to use the CSS instead of a CDW, (2) the CDW was deficient, and (3) the Government exceeded the scope of the CDW when carrying out its investigation. Moreover, Tutis argues that where the Tutis cell phone was in his home, the Fourth Amendment provides enhanced protection from the alleged electronic intrusion. The Government argues in response that the CDW is the functional equivalent to a search warrant because it satisfies the federal requirements for a search warrant, and alternatively that even if there were a deficiency in the CDW, the evidence obtained from Defendant should not be excluded because investigators acted in good faith. The Government does

not deny that its use of a CSS was a search under the Fourth Amendment, but it argues that it obtained a proper warrant under federal and state law.[5]

According to the Supreme Court, a search warrant complies with the Fourth Amendment when it meets three criteria: (1) it was issued by a neutral and detached magistrate; (2) it was based on a showing of "probable cause" to believe that "the evidence sought will aid in a particular apprehension or conviction for a particular offense," and (3) it satisfies the particularity requirement. Dalia v. United States, 441 U.S. 238, 255 (1979). The parties do not dispute that Judge DeLury was a neutral magistrate, so the Court will focus on the remaining two criteria.

a. Probable Cause

There was a substantial basis for Judge DeLury's finding that there was probable cause under the CDW. The Government notes that by October 14, the roving wiretap on Tutis's known phones had been in operation for over two weeks, and it had produced more evidence that Tutis had been dropping phones and using multiple phones simultaneously. (Gov't Sur-Reply at 9-10.)

[5] The Court will decide the instant motion based on federal, rather than state law. See United States v. Rickus, 737 F.2d 360, 363-64 (3d Cir. 1984) ("[F]ederal district courts will decide evidence questions in federal criminal cases on the basis of federal, rather than state, law.").

Judge DeLury specifically found that probable cause existed for ACPO to utilize the device in his CDW Order. See Ex. 1 to Gov't Sur-Reply ("Probable Cause having appeared for the entry of this Order.").

Tutis cites to United States v. Lambis, No. 15-734, 2016 WL 3870940 (S.D.N.Y. July 12, 2016) for the proposition that law enforcement needed a search warrant based on probable cause to use the CSS, but that case can be distinguished. There, the DEA employed a cell-site simulator to investigate an international drug-trafficking organization, but only sought a warrant for pen register information and cell site location information ("CSLI") for a target cell phone. Id. at *1. In Lambis, the agents' primary objective in using the CSS was to identify a "specific apartment" of a suspect by pinpointing "the most likely location of the target cell phone" through forcing the phone to transmit "pings" to the CSS. Id. The Court found that the use of the CSS exceeded the scope of the warrant because "[a]bsent a search warrant, the Government may not turn a citizen's cell phone into a tracking device." Id. at *3. Unlike Lambis, however, the CSS here was not used to "ping" a known telephone of Tutis in order to locate him or his particular residence, but only to try to identify other cell phones that Tutis may have been using

("canvassing"). (Gov't Sur-Reply at 4, 13.)[6] Moreover, in Lambis, the CSS was used "to obtain more precise information about the target phone's location [that] was not contemplated by the original warrant application." 2016 WL 3870940 at *3. The court there noted that "[i]f the Government had wished to use a cell-site simulator, it could have obtained a warrant." Id.

In this instant matter, Detective Dorn did contemplate the use of the CSS in the CDW, as he described the equipment in sufficient detail in the Affidavit, despite not actually calling the equipment a "cell-site simulator." See Ex. 1 to Gov't Sur-Reply at ¶ 4A (describing how the "only function" of equipment would be used to obtain ESN, MSISDN, and IMSI information, and that it would "not be used to obtain any written or oral communications"); id. (describing the way in which the CSS would obtain the data points); id. at ¶ 9 ("I will utilize this technology in an effort to identify additional telephone facility numbers being utilized by [Tutis] or telephone facility numbers that he may utilize during the period of the requested interception."). It was well documented prior to October 14th, 2014, and summarized in the Affidavit, that Tutis was engaged in

[6] The Government alleges that the CSS was used on a particular date to "canvass" several locations where defendant was located, in an attempt to determine the IMSI and/or mobile station ID of the phone(s) Tutis had in his possession. The Government turned over investigation documents regarding the use of the CSS in this investigation. (See Ex. 3 to Gov't Sur-Reply.)

illegal drug transactions through the use of numerous cell phones and that the numbers of some of those phones could not be determined as he continually switched and added cell phones. The Affidavit therefore establishes a "fair probability" that locating the additional cell phone numbers would lead to evidence of a crime. See United States v. Gatson, No. 13-705, 2014 WL 7182275 (D.N.J. Dec. 16, 2014) (denying defendant's motion to suppress where state law enforcement obtained a court-authorized CDW supported by a showing of probable cause for all cell phone GPS data).

b. Particularity of CDW

The Fourth Amendment requires all warrants to contain a "particular description" of the items to be seized. Doe v. Groody, 361 F.3d 232, 239 (3d. Cir 2004). This requirement invalidates "general warrants"--or warrants that "vest the executing officers with unbridled discretion to conduct an exploratory rummaging through [defendant's] papers in search of criminal evidence." United States v. Ninety–Two Thousand Four Hundred Twenty–Two Dollars & Fifty–Seven Cents ($92,422.57), 307 F.3d 137, 149 (3d Cir. 2002) (quoting United States v. Christine, 687 F.2d 749, 753 (3d Cir. 1982)). As now discussed, the Court finds the CDW met the requirement for reasonable particularity of the items to be seized, namely, the electronic

signals containing the identifiers of cell phones in Tutis's near proximity.

The Government argues that the CDW included a "rather detailed description" of how the equipment would be utilized, and relies on United States v. Rigmaiden, 2013 WL 1932800 (D. Az. May 8, 2013) to demonstrate that the CDW did not need to include more specific details about the use of the CSS in order to satisfy the particularity requirement. (Gov't Sur-Reply at 11, Ex. 1 at ¶ 4A.)[7] In that case, the Government located and arrested the defendant, who devised a scheme to obtain fraudulent tax refunds, through a CSS that tracked the location of an aircard connected to his laptop computer. 2013 WL 1932800 at *1. In holding that the warrant obtained for that search was sufficiently particular, the court in Rigmaiden explained that "[t]here is no legal requirement that a search warrant specify the precise manner in which the search is to be executed," and "[t]here is no precedent suggesting that the agent was required to include in his warrant application technical details about the operation of the mobile tracking device." Id. at *16-*17,

[7] ¶ 4A of the Affidavit notes that law enforcement can retrieve additional numbers "by utilizing the equipment in close proximity to [Tutis] at different geographical locations." Later, the CDW notes that the ACPO and FBI "presently have access to equipment that is capable of retrieving the Electronic Serial Numbers and/or International Subscriber Identity Numbers from wireless telephones facilities." (Ex. 1 to Gov't Sur-Reply.)

*32. As a result, in that case, even though the warrant did not disclose that the CSS would capture signals from other cell phones and aircards in the area of Defendant's apartment, this was a "detail of execution which need not be specified under Dalia." Id. at *20. Similarly, in the instant matter, it was not necessary for the Government to include a detailed description in the CDW of how the CSS technology worked. While it might have been helpful to include the words "cell-site simulator" in the warrant and attach instruction manuals, that is simply not required under the Fourth Amendment.[8] The Government's application sufficiently described the device's capabilities, what it would do in terms of receiving electronic signals from cell phones in all directions, and what it would not do in terms of not intercepting communications on such cell phones. The CDW reflected those understandings and limitations.

Next, Tutis explores the distinction between the word "retrieve," which the CDW Affidavit and warrant use frequently, and "interception," which is a different concept in that it

[8] Nonetheless, the Court shares Defendant Tutis's concern about how the "use of a [CSS] must be strictly overseen by the courts due to the invasion of privacy of the home." (Reply Br. at 19.) While the inner workings of this new technology are difficult to obtain, see In the Matter of the Application, 2015 WL 6871289 at *1 (noting that the manufacturers of CSSs are "extremely protective about information regarding its device"), the Court has thoroughly reviewed the various submissions to Judge DeLury and finds that they conform to the requirements of the Fourth Amendment.

"implies the real time seizure of evidence or information in the manner in which it was done in this case." (Def. CSS Reply at 3-4.) As a result, he argues that the CDW "simply does not contemplate the real time 'capture' of information from the defendant's cell phone while he was in his home or place of business." (Id. at 3.) This distinction is insignificant, as the Affidavit and CDW read as a whole make clear what the equipment was intended to do and how it would do it, despite not employing Defendant's preferred choice of words in every instance. According to the Affidavit, the CSS would obtain the ESN, MSISDN, and IMSI from each device, which, as "electronic identifying numbers assigned to a specific cellular facility," are fixed characteristics of a cell phone. (Ex. 1 to Gov't Sur-Reply ¶ 4A); see United States v. Oliva, 705 F.3d 390, 396 n. 4 (9th Cir. 2012) (explaining that an ESN "is a unique number hardwired into every cell phone" and that IMSI numbers are the "unique identifying numbers assigned to the computer chips installed on cellular phones" (citations omitted)); State v. Alexander, 2014 WL 6991736 at *2 (N.J. Super. Dec. 12, 2014) (noting that the MSISDN "is a phone number that is assigned to a particular SIM card"). The purpose of using the CSS was specifically stated in the CDW –- to obtain ESN, MSISDN, and ISMI numbers from phones used by Tutis (see CDW Order at 1-2), and this same purpose was specifically stated in the Affidavit.

(Ex. 1 to Gov't Sur-Reply ¶ 4A, ¶ 9.) Thus, retrieval of the numbers as described in the Affidavit and CDW is a fair characterization of CSS's use here. The authorizing judge was not misled and would have no ambiguity about what he was authorizing in the CDW.

Defendant further argues that the CDW did not satisfy the particularity requirement of a valid search warrant because it did not authorize any search of the defendant's home, or particularly describe the place to be searched, despite the fact that Detective Dorn was "well aware" of Tutis's residence and place of business. (Reply Br. at 7.) The Fourth Amendment specifies only two matters that the warrant must particularly describe: "the place to be searched" and "the persons or things to be seized." United States v. Grubbs, 547 U.S. 90, 97 (2006). As the Government notes, the CSS "emitted a signal omnidirectionally, so that it could be picked up by cell phones in the general vicinity" of the location of the CSS, including any nearby place at which Tutis was observed. (Gov't Sur-Reply at 14.) And in the affidavit applying for the CDW, Detective Dorn explains that in order to "ascertain[] the additional cellular telephone facilities utilized" by Tutis, ACPO would utilize "the equipment in close proximity to [Tutis] at different geographical locations." (Ex. 1 to Gov't Sur-Reply ¶ 4A.) It was clear not only that the CSS would be used at

different locations where Tutis was located, but also that it was necessary to do so in order to determine which cell device(s) were in Tutis's possession as he moved about from place to place. This CSS device was used for the limited purpose of obtaining electronic signals from which one might deduce the identifying data of additional cell phones used by Tutis, and the CDW was very clear about its intended purpose. The CSS was not to be used as a tracking device as in Lambis, or to extract any content from the phones. It was not directed at any known cell phone. It was collecting electronic signals of the very type emitted by all cell phones as they keep in touch with the nearest cell tower or, in this case, the nearest cell-site simulator. It would be used only in "close proximity" of a place where Tutis was known to be. Thus, given "the nature of the crime and the limitation on the items to be searched," the Court concludes that the CDW was sufficiently particular for Fourth Amendment purposes. United States v. Yusuf, 461 F.3d 374, 395 (3d Cir. 2006).

That the CSS could be used near Tutis's home or business, and the notion that the search of a home is subject to stringent restraints, does not alter the result. It is acknowledged that the CSS was deployed in the vicinity of Tutis's home and his

business.[9] The nature of the intrusion into Tutis's home was slight and it was shared with the incidental intrusion into other buildings in the near vicinity: namely, the CSS emitted a wireless signal simulating a cell tower and thereby "inviting" all operating cell phones to make contact electronically. The CSS merely activates a signal inviting nearby cell phones to identify themselves. Whether a Tutis cell phone is on a sidewalk, in a restaurant, or in a home does not change the user's expectation of privacy because the cell phone will make the same response and reveal its existence to the cell tower so long as it is in operating mode. If the device is "off," there will be no signal to the cell tower. The CSS, according to the Dorn Affidavit, would invite its electronic signal exchange only from active cell phones; if in the home one did not wish to communicate identifying data, one need only turn the cell phone off. Where a court has authorized the use of the CSS device for

[9] The Government stipulated at oral argument that its use of the CSS was a search of Tutis's home and business, but claims that it was a valid search under the Fourth Amendment because it properly obtained a warrant. See Sept. 27, 2016 Tr. 10: 4-6 ("We concede for the purposes of this debate, that law enforcement needed a warrant. We got a warrant.") As noted previously, the CDW was not used to seize any cell phone or to seize any communication – it was only used to seize data that identifies the existence of the phone and nothing more. Moreover, Kyllo v. United States, 533 U.S. 27 (2001), which Defendant cites to in his briefing, is inapposite because there, law enforcement failed to obtain a warrant to use the thermal-imaging device. Id. at 40.

the limited purpose of obtaining electronic identifiers from cell phones within the vicinity of the targeted individual, any intrusion by the CSS's electronic signal into the home is both de minimis and reasonable under the Fourth Amendment.

c. Good Faith

Finally, even assuming arguendo that the CDW in this case was invalid due to a lack of probable cause or particularity, the Court nevertheless would find that the evidence seized pursuant to the CDW should not be suppressed because the good faith exception would apply.

In United States v. Hodge, 246 F.3d 301 (3d Cir. 2001), the court stated that the "test for whether the good faith exception applies is whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." Id. at 307 (quoting United States v. Loy, 191 F.3d 360, 367 (3d Cir. 1999)). The court there continued: "The mere existence of a warrant typically suffices to prove that an officer conducted a search in good faith and justifies application of the good faith exception." Hodge, 246 F.3d at 307-308 (citing United States v. Leon, 468 U.S. 897, 922 (1984) and United States v. Williams, 3 F. 3d 69, 74 (3d Cir. 1999)). Nonetheless, an officer's reliance on a warrant would be unreasonable:

(1) when the magistrate judge issued the warrant in reliance on a deliberately or recklessly false affidavit;

(2) when the magistrate judge abandoned his judicial role and failed to perform his neutral and detached function;

(3) when the warrant was based on an affidavit "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; or

(4) when the warrant was so facially deficient that it failed to particularize the place to be searched or the things to be seized.

Ninety-Two Thousand Four Hundred Twenty-Two Dollars and Fifty-Seven Cents, 307 F.3d at 146 (quoting Williams, 3 F.3d at 74 n. 4).

The Government argues that the good faith exception applies because a "reasonably well trained officer" would not have known that the use of the CSS "was illegal despite the magistrate's authorization." (Gov't Sur-Reply at 16-17.) Tutis argues that the good faith exception does not apply because "Detective Dorn did everything possible to hide from Judge DeLury his intention to use a cell-site simulator," because it is not mentioned in the Affidavit or warrant, he used the word "retrieve" as opposed to "intercept,"[10] and only mentioned once in the Friday Reports that he was using a "sensitive technique." (Def. CSS Reply at 11.) As a result, the "only conceivable basis" for failing to

[10] Tutis argues that the CDW misled Judge DeLury into believing that it was a seizure of post-transmission information versus the real-time interception of information.

specify the intention to use a CSS was "to mislead Judge DeLury" into thinking that the CDW was not intended for the interception of identifying information regarding Tutis. (Id.)

Defendant's argument that the Dorn Affidavit applying for the CDW was misleading is not persuasive. While the Affidavit does not explicitly mention the term "cell-site simulator," it does disclose (1) that ACPO was going to use "wireless interrogation equipment," (2) how the device would be used in collecting the data, (3) how the device would not be used, in that it would not be used to obtain any written or oral communications, (4) that its only function would be to identify the electronic signals unique to Tutis's phones, and (5) that ACPO would go to multiple locations known to be frequented by Tutis, based upon a belief that he was dealing drugs and using multiple cellular devices. (Ex. 1 to Gov't Sur-Reply.)

Furthermore, defense counsel properly conceded at oral argument that the Affidavit did not call for, and ACPO did not collect, information about incoming or outgoing numbers from Tutis's phone. (Sept. 27, 2016 Tr. 14: 14-16.) Like Rigmaiden, where the court was persuaded that "agents were using a relatively new technology, and they faced a lack of legal precedent regarding the proper form of a warrant to obtain the location information they sought," here, the ACPO officers likely thought that the CDW was the best way to proceed in using

a CSS under New Jersey law. 2013 WL 1932800 at *31; see also United States v. Wellman, No. 08-0043, 2009 WL 37184, at *7 n. 8 (S.D.W.Va. Jan. 7, 2009) (explaining that "law enforcement officers utilizing relatively new technology and innovative techniques in good faith should not be penalized with suppression of important evidence simply because they are at the beginning of a learning curve and have not yet been apprised of the preferences of courts on novel questions"). Moreover, in September and October 2014, when Judge DeLury approved the roving wiretap and CDW at issue, courts and other stakeholders had just begun to opine on the issue of cell-site simulators and their Fourth Amendment implications. The Department of Justice did not release its policy requiring agencies wishing to use a CSS to obtain a search warrant supported by probable cause until September 2015. Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (Sept. 3, 2015), http://www.justice.gov/opa/file/767321/ download. Indeed, the first federal court decision to suppress evidence obtained by CSS for lack of a search warrant did not occur until July 2016, in the Lambis case, 2016 WL 3870940, which is in any event addressing circumstances quite different from the present case, as discussed above. Additionally, New Jersey courts have not yet opined on the constitutionality of cell-site simulators. As a result, the ACPO officers should not be penalized for

obtaining a CDW in October 2014 that explains how the CSS would work for the limited purpose of obtaining additional cell phone identifiers that through process of elimination would lead to the number for Tutis's new cell phone(s). This is not a case like Lambis where officers used a CSS "not contemplated by the original warrant application" – here, law enforcement obtained a CDW, which, as explained infra, under state law, is equivalent to a search warrant, and which, as determined above, satisfied the Fourth Amendment's requirement for a search warrant.

d. A Communications Data Warrant is Equivalent to a Search Warrant Under State Law

Finally, the Government argues that under New Jersey law, a CDW, not a search warrant, was the proper vehicle for the authorization to use a CSS; thus, there is no basis for suppression. Defendant argues that the CDW did not rise to the level of a search warrant and thus did not authorize the use of a CSS under New Jersey law because the New Jersey Wiretap Act does not mention the use of a CSS, and a search warrant is required because "there is simply no case in which a CSS was used when authorized by a CDW." (Def. CSS Reply at 10.)

The New Jersey Supreme Court has recently instructed that a communications data warrant is "the equivalent of a search warrant." State v. Lunsford, 226 N.J. 129, 133 (2016). Given that New Jersey law enforcement's use of CDWs are not well known

to the public, the Government has explained to the Court that the State of New Jersey uses CDWs instead of search warrants to make recordkeeping easier to deal with, and to ensure that only specially-trained judges issue the warrants. (Gov't Sur-Reply at 19, n. 11.) The Government notes that New Jersey law enforcement obtained a September 2013 CDW authorizing the use of a CSS, so this demonstrates that prior to the Tutis CDW, the "proper procedural vehicle" to apply for authorization to use a CSS was indeed a CDW. (Id.)[11] The Government also submitted an August 1999 Directive ("Directive 9-99") called "Procedures to be Followed in Handling Applications for Communications Data Warrants and Communications Information Order." (Ex. 4 to Gov't Sur-Reply.) While the Directive does not define a CDW, it does explain that "the standard to be applied in deciding communications data warrant applications is that of probable cause." (Id.) Thus, since both a CDW and a search warrant require a showing and finding of probable cause, there is "no material difference" between them under the Fourth Amendment. (Id. at 20-21, n. 13.)

[11] The Government further notes that "[g]iven that a CSS will be utilized in a number of locations to try to locate cell phone(s), the difficulties in drafting a search warrant authorizing the use of a CSS, when a search warrant normally is used to search a particular location, make it obvious why the ACPO used the procedural mechanism of a CDW, rather than a search warrant, to obtain authorization to use a CSS." (CSS Sur-Reply at 20, n. 13.)

Additionally, Defendant argues that CDWs under state law can only be used to obtain stored electronic records, but the Government responds that nothing in the New Jersey wiretap statute limits the use of a CDW to stored electronic records. (Id. at 22; Def. CSS Reply Br. at 10.) Defendant relies on State v. Finesmith, 408 N.J. Super. 206, 208 (App. Div. 2009) for the proposition that a "CDW is directed to acquisition of post-transmission electronic storage kept by an electronic communication service or remote computing service for reasons of backup protection for the communication." But other courts interpreting New Jersey law have noted that a CDW can be used for interception of a communication contemporaneous with transmission. See, e.g., Badillo v. Stopko, No. 11-4815, 2012 WL 1565303 at *1 (D.N.J. May 2, 2012) ("intercepts of telephone calls through Communications Data Warrants"); State v. Edwards, 2011 WL 1466152 at *1 (N.J. Super. Apr. 19, 2011) ("[T]elephone conversations were intercepted and recorded pursuant to a communications data warrant issued by a Superior Court Judge."). Given the current practices of New Jersey law enforcement, the lack of precision in the New Jersey wiretap statute, and the uncertainty in the caselaw regarding this issue, the Court therefore finds persuasive the Government's argument that nothing limits the use of a CDW to obtaining stored electronic records and information.

III. MOTION FOR A BILL OF PARTICULARS BY JAZMIN VEGA

Jazmin Vega argues that there is insufficient information in the Indictment and in discovery to put her on notice as to exactly what the Government is alluding to regarding her drug involvement; thus, she asks the Government to provide her with a bill of particulars. A bill of particulars is "[a] formal, detailed statement of the claims or charges brought by a plaintiff or a prosecutor, usu[ally] filed in response to the defendant's request for a more specific complaint." Black's Law Dictionary (10th ed. 2014). See N. Jersey Media Grp. Inc. v. United States, ____ F.3d ____, 2016 WL 4651386 at *6 (3d Cir. Sept. 7, 2016) (noting that a bill of particulars "effectively narrows the government's case at trial in the same way as the formal charging document"). A district court has broad discretion in granting or denying a criminal defendant's motion for a bill of particulars. United States v. Rosa, 891 F.2d 1063, 1066 (3d Cir. 1989). Among the purposes of a bill of particulars is to inform the defendant of the nature of the charges brought against him so that he is able to adequately prepare a defense. United States v. Moyer, 674 F.3d 192, 203 (3d Cir. 2012) (citing United States v. Addonizio, 451 F.2d 49, 63 (3d Cir. 1971)).

A district court should only grant a motion seeking a bill of particulars when an indictment's failure to provide factual

or legal information "significantly impairs the defendant's ability to prepare his defense or is likely to lead to prejudicial surprise at trial." Rosa, 891 F.2d at 1066. However, a defendant is not entitled to general discovery of the government's case, evidence or witnesses. United States v. Armocida, 515 F.2d 49, 54 (3d Cir. 1975)). In ruling on a request for a bill of particulars, a court should consider all information that has been disclosed to a defendant in the course of the prosecution, whether or not included in the indictment. United States v. Kenny, 462 F.2d 1205, 1212 (3d Cir. 1972).

A bill of particulars is not appropriate in a case such as this, where Defendant Vega has been given substantial access to discovery. United States v. Urban, 404 F.3d 754, 772 (3d Cir. 2005) ("[A]ccess to discovery further weakens the case for a bill of particulars."). While she claims that she will be "lost in a sea of accounting and business transactions, conversations with co-workers and relatives, and literally thousands of documents without having any idea which of these are alleged to constitute crimes against" her, she omits the extensive discovery that the Government has already provided to her. (Def. Br. at 3.) This primarily includes (1) a "show and tell" meeting where the Government has already explained the case to her and her attorney and disclosed what the Government regards as substantial evidence of criminality, (2) an exhibit list

where Vega can identify the conversations in which she participated which the Government seeks to use at trial, (3) various demonstrative exhibits, and (4) recorded conversations pursuant to wiretaps, among other items. (Gov't Br. at 6.)

The Superseding Indictment and Second Superseding Indictment combined with this extensive discovery already disclosed to Vega provides her with more than sufficient information to understand the nature of the charges against her, prepare her defenses, and to avoid surprise at trial. The Court therefore finds that Defendant Vega has sufficient information from the Government to know what she is charged with and to prepare for trial, and it will not require the Government to particularize all of its evidence. Vega's request for a bill of particulars is therefore denied.

IV. CONCLUSION

For all of these reasons, Defendant Tutis's motion to suppress evidence obtained by deploying the cell-site simulator pursuant to the October 14, 2014 CDW, as well as Defendant Vega's motion for a bill of particulars will be denied. An accompanying Order will be entered.

October 20, 2016
Date

s/ Jerome B. Simandle
JEROME B. SIMANDLE
Chief U.S. District Judge